DIGITALEUROPE

DIGITALEUROPE'S INPUT ON INTERNATIONAL DATA TRANSFERS UNDER THE GDPR (FABLAB CONFERENCE)

Brussels, 8 December 2017

KEY MESSAGES

On 18 October 2017, the Article 29 Working Party (WP29) organized its regular FabLab event on the General Data Protection Regulation (GDPR). The event had two sessions (1) on the international data transfers and (2) on transparency under the GDPR.

DIGITALEUROPE responds to the questionnaire sent to stakeholders ahead of the international data transfers session, raising few key aspects for further consideration:

1. Chapter V "Transfers of personal data to third countries or international organisations" could benefit from **further clarification and simplification of the rules**;
2. Adequacy decisions should **focus on the outcome rather than the content**; hence, couldn't be solely based on GDPR;
3. **EU diplomatic toolbox** should be used to (1) **strengthen the slow progress of the development of international norms** and (2) **address the wide-ranging powers on national intelligence agencies**;
4. **Access mechanisms differ from transfer mechanisms**;
5. **Certification methodology needs to be both agile and robust**, and it should certify a minimum set of requirements for a Privacy Program. It should also **leverage international experience around certification**.

DIGITALEUROPE supports the efforts to increase the dialogue with stakeholders throughout the GDPR implementation process.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

International transfers in general

1. The GDPR provides a tool box for framing data transfers abroad: does this list answer your needs and expectations? What type of guidelines would you like to see developed by the WP29 on those tools? Are there specific topics where you need guidance on?

We welcome strong privacy rules and believe that improvements on the guidance side would support this objective. The list and corresponding WP29 activities on chapter V should not become a tool for extra judicial implementation of what was proposed by the legislators nor anticipate future European Court of Justice (ECJ) rulings and cater for all policy objectives envisioned by European legislators as expressed in recital 4.

'The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.'

However, the continued uncertainty around international data transfers and in the case when a transfer made in accordance with General Data Protection Regulation (GDPR) is suddenly deemed illegal, how much time a controller will have to react. It seems only ECJ has the power to create certainty, not the legislators nor the Data Protection Authority (DPA). However, if such ECJ decision is made, WP29 should, in cooperation with the industry, develop a mechanism for well-intended companies to adjust and comply with the new realities. At the same time, it should be recognised that European based multinationals have complex IT systems and global reach. This means that technical and operational adjustments will take, and in many cases, depend on how suppliers of IT and software can introduce new software upgrades.

Consideration should also be given to the risk of bottle neck of a sudden surge in the demand of IT integration consultants if European based companies at a given point in time need to make fundamental changes.

From a European processor perspective, the GDPR doesn't provide for more workable solutions than the current legal framework. The problem is still that there are no processor to processor standard contractual clauses (SCCs). Instead, European processors need to find solutions for their customers (controllers) to directly enter in SCCs with non-European (sub-) processors. While current interpretations permit a European processor to represent its customer (controllers) per power of attorney towards (sub-) processors, the opposite model, by which the European processor would represent the non-EU (sub-) processors towards the customers, is generally not accepted.

But in practice, the requirement to represent the customers towards the (sub-) processors causes a lot of administrative work. For instance, a different set of standard agreements must to be concluded for every customer. It would be much more efficient for the processor to be able to represent the (sub-) processors towards the customers as he would only need one power of attorney for many customers. And the result would be the same.

The SCCs for standard cloud services will look the same, per definition ("standard") for each and every customer. Therefore, there is the need to foster simple methods of entering into the standard contractual clauses, e.g. accession models, workable processor to processor SCCs.

Ultimately, we want the current data transfers mechanisms like SCCs to continue to be a viable option. It is worth noting that transfers are not exclusively going from the EU directly to the US. We are global companies and our transfers go all over the world. Equally, a single harmonized way of transferring data from the EU in jurisdictions across the world, such as Privacy Shield is where we should be going.

2. How to better communicate to the individuals on the guarantees offered and individual's rights in the context of international transfers? How to make privacy policies clearer about international transfers taking into consideration the transparency requirements regarding international transfers as set out by the GDPR?

Articles 13 and 14 are clear when it comes to communication and nothing further is needed.

Adequacy

1. What are the core commercial and law enforcement principles that you would consider necessary to be found in a third country legislation for it to be considered as offering an adequate level of protection (e.g. "new" data subject rights, DPIA etc.)?

Adequacy decisions based on GDPR per se are not a European law enforcement practice. Consequently, it is of critical essence to avoid a situation where adequacy decision is making a judgement about a third country's privacy regime based on GDPR. Such scenario would be seen as a double standard, ultimately undermining the legitimacy of the European privacy regime.

Furthermore, for third countries' data protection laws, the adequacy decision process should focus on outcome and not content. An adequate level of protection is not necessarily ensured by provisions in third countries' law when mirroring the GDPR but rather by principles and requirements that result to the desired level of adequate protection for data subjects.

Need for clarification

Although the adequacy has had some success in imposing European privacy standards on third countries, a more effective way to extend these to citizens of third countries is to secure a predicable regime of inbound data transfers from third-countries to Europe, hereby extending European privacy standards to third countries' citizens. This accomplishment will also stimulate investments and job creation in European based data processing, a clear but still yet unaddressed opportunity by policy makers. The reason for this is that adequacy decisions foster predictability of only outbound data transfer from EU to third counties, which ultimately provides incentives to European based data processors to move data processing outside Europe. While at the same time adequacy offers no predictability for inbound data transfers from third countries to process such data in European. A reciprocal adequacy decision meaning that EU and third country makes two unilateral adequacy decisions to secure data flows in both directions, still lack certainty as such decisions can be unilaterally withdrawn.

Contrary to adequacy, securing data flows in FTA (Foreign Trade Agreement) will provide European data processers with the necessary certainty to process third country citizen's personal data in Europe, promoting investments and jobs in Europe. At the same time, third country citizens will benefit from European privacy

standard. Predictable rules for inbound data transfers to Europe, which can be assured in a predictable way and on a mass scale through FTA. Such outcome would build on top of the scale of European market while increasing further the scale of European based processing operations, gaining even larger scale of operation by having predictable inbound data transfers rules to rely on. This is the opportunity that European based industry is still waiting for to make the policy claim that "privacy can be a competitive advantage".

2. From a company's perspective what (additional) technical or organizational measures can be taken to effectively limit access to personal data from law enforcement and intelligence agencies in the third country to the extent absolutely necessary in a democratic society?

Encryption provides for an additional layer of protection but full encryption is not feasible in each and every constellation. Encryption keys should be with the controller so that the processor can't be subject to any demand to hand over unencrypted data.

European policy makers should ensure increased focus and resources in cPPP (Cybersecurity Public Private Partnership) on quantum safe software programming. This will improve the capabilities of European software companies needed to increase resilience against possible aggressive uses of quantum computing1.

Regarding third countries law-enforcement and intelligence agencies, it should be clear that GDPR is not the proper mechanism to address surveillance practices' issues. In terms of law-enforcement, more countries should sign up to the Budapest convention. This mechanism should receive more attention in driving material improvements for citizens privacy in and outside Europe. Regarding the intelligence agencies, EU should increase efforts through e.g. the EU diplomatic toolbox to (1) strengthen the slow progress of the development of international norms[2] and (2) addressed wide ranging powers on national intelligence agencies[3]. Furthermore, some countries are proposing wide ranging obligations on European companies to disclose their source code that will introduce new threats for European citizens and businesses4. One way to limit this threat is to include prohibition, without exceptions, of source code disclosure for ICT products used for civilian purposes, in FTA governing data transfers, such as in the ongoing NAFTA renegotiation[5].

Binding Corporate Rules (BCRs)

1. How to improve the BCRs and their process of validation by the DPA?

General standard modules and agreed clauses should be developed, so they can easily be re-used. Furthermore, at a time when DPAs are strained in terms of resources while more companies are applying for BCRs, we urge data protection authorities to ensure that they will be able to efficiently deal with applications. This is paramount for the mechanism to continue to be an effective option for companies and to increasingly become a smoother and faster process. In that regard, making the requirements for controllers and processors more consistent, and speeding up the process would help.

[1] See http://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility
[2] See https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges
[3] See http://www.mannheimerswartling.se/globalassets/publikationer/national-intelligence-law.pdf
[4] See https://www.recordedfuture.com/china-cybersecurity-law/
[5] See page 9 https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf

2. The GDPR provides that BCRs can be adopted not only by a group of undertakings but also by groups of enterprises engaged in a "joint economic activity". In your view, what elements should be considered to assess whether a group of companies are engaged in a "joint economic activity"?

It shouldn't be necessary to have a joint economic purpose but to have a certain stability in a data processing relationship which is about to last. Long standing business relationship leading to stable data processing terms and conditions (relationships) – example: cloud services with the same sub-processors. The starting point shouldn't be comparable business models, but rather long standing and stable business relationships.

The "joint economic activity" could fall under 2 different scenarios: On the first one members of the BCR under "Joint Economic Activity" need to define if all entities have decision making on the data. If they do the requirements should fall under Article 26 (as those entities all make decisions on the use of data).

A second scenario would be when one entity who is BCR certified can open their BCR for either its supply chain or distributor network to operate under the umbrella of said approved BCR. WP29 could, with inputs from industry, determine a minimum set of compliance requirements that the supply chain or distribution network would need to demonstrate in order to be able to transfer data under the existing BCR. Amongst other articles this could also satisfy the requirements of Article 28.1 of the GDPR.

A separate but related issue that needs to be addressed relates to business being done by two companies who hold a BCR. Greater flexibility should be granted to companies with joint economic activity when both have demonstrated robust data protection practices; this should be an asset for the two companies that have undergone the BCR process.

3. To ensure the bindingness of BCRs for each participating entity, already approved BCRs mainly make use of intra-group agreements and where possible unilateral undertakings. Which other instruments could be taken into account in this perspective?

Accession models (see answer above). We believe the Intercompany agreements are sufficient to achieve the BCR objectives. They are not the easiest of mechanisms to implement, but provide a greater degree of certainty.

4. What guarantees could be provided when the applicable legislation of a third country prevents the company/entity from fulfilling its obligations under the BCRs?

To the extent that a company entity can't meet its obligations under the BCRs it must be excluded from processing data under the BCR.

The only real topic to fall under this category is government access to information. This is a government to government issue and needs to be resolved at the supranational or diplomatic level. No transfer mechanism could solve this but experience shows that companies will make efforts to the best of the abilities and without compromising compliance with other countries laws to protect data. Beyond that, there is no magic bullet to solve the issue from the company side.

5. In your view, are BCRs only a tool for transfers or more generally a tool for achieving compliance?

Whereas BCRs are in principle designed as a tool for transfers, they are increasingly becoming a useful tool - not for but- towards compliance. We do not see BCRs as a tool for compliance. Many companies that don't have the resources to go through the approval process or the structure which makes BCRs attractive in the first place. Such an approach would also undermine the attractiveness of other mechanisms for transfers. And

importantly, it would move us away from the accountability principle of the GDPR by reintroducing a system of approvals and authorisations for compliance.

However, we believe that companies that have BCR approvals have satisfactorily demonstrated compliance and accountability towards the authorities; in order to obtain a BCR you need to demonstrate accountability and a robust data protection program. This is rigorous and not a self-assessment, so without a complete program it can't be achieved. Transferring might be the ultimate motivation, but a robust program is the basis for it, thus achieving compliance is necessary.

And it is, finally, important to note that BCRs are also attractive from a competitive and business perspective; companies that have BCR approvals are considered in the market place to have a good level of compliance.

Derogations

1. What should the information provided to the data subject include in case of a transfer based on the derogation of consent? Information on data recipients or categories of recipients, countries to which the transfer is being made, level of data protection and specific privacy risks in the third country etc.?

We believe that as data subjects' awareness continues to increase, explicit consent may become a more reliable basis for transfers. Practically it can be counter-productive to overload the data subject with too much or too complex information. We believe that each individual company should assess the type and detail of information that can achieve the outcome required in Article 49 i.e. informing the data subject "of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".

Data access is different from a data transfer

It is of outmost importance for the development of European data processing industry to be able to provide services from Europe. A concrete opportunity to further improve the European conditions is using the derogations section on data transfers in GDPR. But more clarification is required.

European based data processing is dependent on the need to secure possibility to access data to and from EU in a very specific context, that does not include a permanent transfer or a bulk transfer of personal data that is incidental and there is not an intention/purpose to process personal data for value extraction. Specifically, in the business to business (B2B) context, where privacy trained personnel, under an established contractual relationship and with technical mitigation procedures in place such as VPN and encryption, need to access remotely information in IT systems for pure maintenance, software update or incident support management purposes. It is of absolute essence that such situations are addressed in an effective manner where European businesses are through certification or Code of Conduct able to benefit from such an access-mechanism without the need to repeatedly inform or await a decision from a DPA.

Certification

1. In your view, what are the advantages and disadvantages of certification as a tool for transfers?

Our comments reflect the definition of certification as foreseen under Art 42 of the GDPR (leaving aside codes of conduct as defined under Art 40).

Certificates provide market incentives by creating transparency and trust and, as a result, offer competitive advantages for the services inspected. Certificates provide an efficient way for users to inform themselves and to compare offerings.

In addition, certification is an essential tool to demonstrate and document compliance. However, it is important that the certificate is valid throughout all EU member states in order to establish legal certainty and enhance the internal market.

A horizontal certification procedure to manage permanent data transfers to third countries should be developed in a joint effort including representatives from European businesses. Such certificates could be tailor made for specific situations such as European based Multination Enterprises, whose conditions are significantly different (complex and large IT systems, as well as vast geographical footprint outside EU).

Certifications could have the advantage of scale vs other mechanisms such as BCR's. Certifications should be done by accountability agents and do not require regulators' review. The certification methodology needs to be both agile and robust, but is should also go beyond just transfers. It should certify a minimum set of requirements for a Privacy Program.

Certifications should also be a way to satisfy Art. 28.1 requirements. Large companies may have tens of thousands of suppliers and making sure that only processors providing "sufficient guarantees to implement appropriate technical and organizational measures" are used is an extremely time and resources consuming process. A quick set up of certifications for this purpose should be a priority. If existing certifications can be used (even from other regions) to ensure this, it should be an avenue to be explored with the upmost urgency.

In addition, there is need to differentiate between certifications (a minimum standard) and BCR's (a higher standard) as the latter require much more effort and a robust Data Protection program. This implies a lengthy demonstration process in front of a regulator with peer review by two additional regulators. The benefits for BCR achievement should be higher than mere transfers.

2. What tools should be established by the WP29 to facilitate the development of certification as a tool for transfers?

Develop clear standards as underlying requirements against which a certificate can be provided. DPA's shouldn't certify themselves, but remain at the control level.

There might be temptation to align privacy certifications with other type of certifications that require conformity assessment and technical skills. This should be avoided as it will increase the cost of certification and limit the number of possible accountability agents (Certification bodies). If we limit the number of accountability agents, we will inevitably increase the cost and limit the access to certification.

As for tools, WP29 should try to leverage international experience around certification. The APEC Cross Border Privacy Rules (CBPR) system and Privacy Recognition for Processors (PRP) certification process is a good example of a minimum set of requirements that can be applied by privacy centred accountability agents. WP29 should avoid reinventing the wheel and learn from existing international experience.

In addition, WP29 should be open to allowing other existing certification schemes from outside the EU to be used to demonstrate compliance. The territorial scope in article 3 makes it imperative to allow companies doing business in the EU (e.g. processing EU data subjects' personal data via a website) to certify outside of the EU. Similarly, if trends hold, EU companies will eventually need to get certifications to transfer data an operate in other countries that might place similar restrictions in their territory (i.e. Japan). Interoperability of

certification mechanisms will become imperative if trade barriers are to be avoided and for e-commerce to grow.

ADDITIONAL QUESTIONS

International transfers in general

1. What is, in your view, a "transfer"?

A transfer is the act of making data accessible to a third party, constitutes an overly broad conceptualization of temporal data access. A data access for temporal purposes in a B2B established relationship where the purpose to access data is not to make a permanent transfer nor to process personal data for any other purposes than pure technical maintenance/support should not be conflated with permanent bulk data transfers where the purpose is to process data to extract value. In addition, commissioning a data processor based on a solid data transferring agreement (along the lines of the GDPR) should not be considered transfer to a third party. The data processor is not a third party.

2. How to apply the principle of privacy by design and privacy by default in the framework of international transfers?

These principles, as well as all principles outlined by the GDPR, must be respected throughout the entire chain of processing.

3. What should be the role of the DPO on international transfers?

The role of the DPO is to work towards achieving compliance for his/her own respective company. But the role doesn't stop there. He/she should be involved in the entire value chain, especially if the company relies on external processing/downstream processing.

4. Where to draw the line between applicable law and international transfers of data under the GDPR? For example, how could a controller located outside the EU but subject to the GDPR according to Article 3.2 (e.g. processing EU data subjects' personal data via a website) frame its transfers back in its country?

In general, there should be no difference regarding the processing and transfer of personal data depending on where the controller is located. In particular, there should not be a disadvantage for controllers located in the EU versus those located outside.

5. How to assess the privacy risk related to the transfer of data outside EU in a DPIA?

Transfer specific privacy risk must be related to the legal situation in the receiving country. It is questionable how an average European controller (which may be an SME) could make a better judgement on this, if the obligations and guarantees stipulated in e.g. SCCs are not regarded as sufficient.

Adequacy

1. In case of onward transfers, which measures do you think can be applied, to make sure that the adequate level of data protection in the third country with an adequacy decision will be expanded to the third country into which the onward transfer takes place?

Check:

- If the transfer goes back to the EU;
- If the transfer goes to country which is considered adequate;
- If the used transfer mechanism is considered adequate (SCCs);
- Whether the requirements for adequacy in article 45 para 2 are fulfilled.

BCRs

1. How could the acceptance by the controller or processor established in the EU of "liability for any breaches of the BCRs by any member concerned not established in the Union" be provided?

This is already done under the current BCR process. That statement is both contained in the BCR documentation provided to DPAs and in the Inter Company Agreement. Therefore, for processors and controllers with BCR this is not a relevant issue. It might be an issue if we were to extend the BCR to companies that are not subsidiaries but acting under "Joint Economic Activity", but that could also be resolved under contract.

2. The GDPR introduces specific requirements for entities acting as processors which must be addressed in a "contract or other legal act" that is binding between the controller and the processor. In the context of BCRs, should such "contract or other legal act" also be an element constituting the BCRs, and be subject to the approval of the DPA?

It should not. That would be overly bureaucratic. Controllers and processors manage thousands or in some cases dozens of thousands of relationships. There is no way that a DPA can have enough bandwidth to provide approval to all of these contracts. Furthermore, BCRs are a demonstration of accountability. There is absolutely no pint in establishing a burdensome control for a company that has demonstrated a robust and accountable Data Protection program.

Derogations

1. Can private entities rely on the public interest derogation, Article 49 (1) (d)?

In exceptional cases, probably yes, as in principle the GDPR allows private entities to rely on public interest but this must respect the principle of proportionality. The public interest must therefore outweigh the interest of the affected data subject in the given case. This may be applicable for transfers of personal data to investigate competition, customs or tax cases.

2. Regarding the derogation of Article 49 (1) (f) what do you consider falls under the wording "physically or legally incapable"? What circumstances fall under legal incapability?

This applies to cases where the data subject is hurt and without consciousness but would otherwise have given consent to the data transfer.

Certification

1. In your view, what exactly should be certified? For instance, should it be a transfer or set of transfers? The processes implemented by an entity? Other elements?

- What should be certified;
- The ability to demonstrate compliance when required by a regulator (Accountability);
- Elements that would enable a controller to meet the requirements of Article 28.1 from by providing minimal requirements for a processor to meet its responsibilities;
- A strong focus should be on achieving the minimum standards under the GDPR through review of the Privacy Programs;
- An incident management system;
- It should be the mechanism and process - not for a single transfer but the overall approach;
- The process as implemented by all entities involved in the processing activity.

2. In your opinion, what should the certification process look like in practice?

The certification procedure should be initiated by means of an application by the certification seeker (CS). Following the submission of an application by the CS or after a contract for the implementation of a certification procedure has been concluded, the responsible accountability agent inspects the service based on a set of predefined inspection requirements. Based on its report, stating that the requirements of the GDPR have been fulfilled, a certificate is to be granted or denied. The certificate must be published by the accountability agent or by another body determined by law (e.g. the DPA). The date of issue and the date on which the validity of the certificate expires must be specified on the certificate.

--
For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 2 609 53 10 or iva.tasheva@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK